REMARKS

Claims 8 to 18 are now pending.

Applicants respectfully request reconsideration of the present application in view of this Amendment.

Applicants respectfully submit that the "final" nature of this Office Action is improper. The First Office Action dated April 29, 2003 rejected claims 1 to 7 and did not reject Applicants' claims 8 to 18. Now, the Second (and Final) Office Action has been made final because, as explained by the Office Action, "Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, this action is made final. See MPEP § 706.07(a)" (all-caps and bold emphasis not included here). This is an incorrect determination. In fact, Applicants did not amend the claims, there are no new grounds of rejection – and instead, there are *new rejections* for different *unamended* claims. MPEP § 706.07(a) states that *"second or any subsequent actions on the merits shall be final, except where the examiner introduces a new ground of rejection that is* ***neither necessitated by applicant's amendment of the claims nor based on information submitted in an information disclosure statement filed during the period*** *set forth in 37 C.F.R. 1.97(c) with the fee set forth in 37 C.F.R. 1.17(p)."* Accordingly, the Office Action of November 19, 2003 ***should be nonfinal***, and Applicants respectfully request such be noted in the Record.

As a final note, it would be incredibly unfair, unjust and contrary to the Patent Rules to suggest that Applicants should have assumed that because canceled claims 1 to 7 (7 claims total, 2 independent claims) were rejected for various reasons, that unidentified and unrejected claims 8 to 18 (11 claims total, 3 independent claims) would be necessarily silently rejected for identical reasons. Thus, Applicants respectfully request removal of the Finality of the Office Action of November 19, 2004.

35 U.S.C. § 103(a) – Shaw and Matyas references

Claims 8 to 11 and 18 were rejected under 35 U.S.C. § 103(a) over U.S. Patent No. 5,425,103 to Shaw ("Shaw reference") in view of U.S. Patent No. 5,142,578 to Matyas et al. ("Matyas reference").

The Shaw reference purportedly concerns a variable-key cryptography system in which binary data is encrypted or decrypted using a final key formed by manipulating one or more user keys and a base key, and combining the manipulated keys using an exclusive-OR operation. Title and Abstract, lines 1-4. According to col. 1, lines 45-49, the user and base

keys are binary sequence having any suitable number of bits, and the maximum length of keys is limited by the capabilities of the software and hardware. The base key is stored in a manner that allows it to be retrieved; the user key is not retained in its original form after inputted. Col. 1, lines 49-54. The Shaw reference indicates that manipulation of the user key involves the steps of permuting the user key, circularly shifting the permuted user key and filling a memory location with one or more copies of the permuted and shifted key such that the result has a length equal to that of the base key, the user's choice of key length is not restricted. Col. 2, lines 8-12 and 52-53.

The Matyas reference purportedly concerns a method and apparatus for securely distributing an initial Data Encryption Algorithm (DEA) key-encrypting key by encrypting a key record – the key record consisting of the key-encrypting key and control information associated with that key-encrypting key – using a public key algorithm and a public key belonging to the intended recipient of the key record. Abstract, lines 1-7. The Matyas reference refers to the type and usage attributes assigned by the originator of the key-encrypting key in the form of a control vector as being cryptographically coupled to the key-encrypting key in the form of a control vector are cryptographically coupled to the key-encrypting key such that the recipient may only use the received key-encrypting key in a manner defined by the key originator. Abstract, lines 16-21.

In contrast, claim 8 is directed to a method for implementing an encryption system including the features of:

> generating a Vernam key via a symmetrical cipher, *the generating being aided by using a secret key and a variable parameter, the Vernam key having a length that is equal to a length of a message to be protected, the secret key having a defined key length, the variable parameter having a length which is a function of the defined key length*;
>
> encrypting, via a Vernam key, the message using logic operations of a Vernam cipher;
>
> *communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher*;
>
> regenerating the Vernam key; and
>
> decrypting the message using the regenerated Vernam key.

The Shaw and Matyas references, alone or in combination (and it is respectfully submitted

that they are not properly combinable), do not teach all of the features of claim 8, including the features of generating a Vernam key via a symmetrical cipher, the generating being aided by using a secret key and a variable parameter, the Vernam key having a length that is equal to a length of a message to be protected, the secret key having a defined key length, the variable parameter having a length which is a function of the defined key length; encrypting, via a Vernam key, the message using logic operations of a Vernam cipher; and communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher; and regenerating the Vernam key, as in claim 8. As the Office Action agrees, the Shaw reference does not disclose (at least) communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher. The Matyas reference does not cure the deficiencies of the Shaw reference. The Office Action cites col. 3, lines 1-27 of the Matyas reference as support. In fact, the Matyas reference at col. 3, lines 1-27 appears to describe 1) distributing one secret DEA key-encrypting key between the originating node and the receiving node, and thereafter transmitting all other DEA keys unthis this common DEA key-encrypting key; and 2) a hybrid system where a public key is transmitted with integrity to a second hybrid cryptographic system. A secret DEA key-encrypting key is generated and encrypted under the public key at the second system and transmitted to the first system – the first system using the corresponding private key to decrypt it and use it to distribute additional DEA keys for use by the first and second systems. Both of these communication schemes do not appear to recite or follow the feature of claim 8, as recited above. Accordingly, the Shaw and Matyas references when combined still lack a feature of claim 8 and therefore do not render claim 8 obvious. Applicants respectfully submit that, in light of the above and the references, claim 8 is allowable and withdrawal of the rejection of claim 8 is respectfully requested. Claims 9 to 11 depend from claim 8 and are thus allowable for at least the same reasons as claim 8. Claim 18 contains features analogous to those of claim 8 and is thus allowable for essentially the same reasons as claim 8.

Withdrawal of the rejection of claims 8 to 11 and 18 under 35 U.S.C. § 103(a) is respectfully requested.

35 U.S.C. § 103(a) – Shaw, Matyas and Maher references

Claims 12 to 17 were rejected under 35 U.S.C. § 103(a) over the Shaw reference in view of the Matyas reference and further in view of U.S. Patent No. 5,513,261 to Maher ("Maher reference").

Claims 12 to 14 depend from claim 8; claims 16 to 17 depend from claim15. Accordingly, claims 12 to 14 are allowable for the same reasons as claim 8 over the Shaw and Matyas references.

The Maher reference purportedly concerns an electronic card for insertion into a host electronic device for providing to the host device security parameters pertaining to the rightful holder of the card. Abstract, lines 1-3. The Maher reference describes that the security parameters are stored in encrypted form to preclude their discovery by unauthorized parties. Abstract, lines 3-5. The Maher reference further describes that the decryption mechanism resists probing by unauthorized parties. Abstract, lines 5-6.

The Maher reference, when taken in combination with the Shaw and Matyas references (even though it is believed the references are not properly combinable), does not teach or suggest at least the feature of communicating, from a sending point to a receiving point, the secret key and the variable parameter via at least one of (A) a secure channel separate from a message-transmission path and (B) the message-transmission path, the message-transmission path being secured via an asymmetrical cipher; and regenerating the Vernam key, as in claim 8 (and thus, claims 12 to 14).

Accordingly, Applicants respectfully submit that claims 12 to 14 are allowable and withdrawal of the rejection of claims 12 to 14 under 35 U.S.C. § 103(a) is requested.

Claim 15, and its dependent claims 16 to 17, contain features analogous to those of claim 8, and are thus allowable for essentially the same reasons as claim 8 over the Shaw, Matyas and Maher references.

Applicable Law

The Federal Circuit in the case of In re Kotzab has made plain that even if a claim concerns a "technologically simple concept" -- which is not even the case here, there still must be some finding as to the "specific understanding or principle within the knowledge of a skilled artisan" that would motivate a person having no knowledge of the claimed subject matter to "make the combination in the manner claimed", stating that:

> In this case, the Examiner and the Board fell into the hindsight trap. The idea of a single sensor controlling multiple valves, as opposed to multiple sensors controlling multiple valves, is a technologically simple concept. **With this simple concept in mind, the Patent and Trademark Office found prior art statements that in the abstract appeared to suggest the claimed limitation. But, there was no finding as to the specific understanding or principle within the knowledge of a skilled artisan that would have motivated one with no knowledge of Kotzab's invention to make the combination in the manner claimed.** In light of our holding of the absence of a motivation to combine the teachings in Evans, we conclude that the Board did not make out a proper *prima facie* case of obviousness in rejecting [the] claims . . . under 35 U.S.C. Section 103(a) over Evans.

(See In re Kotzab, 55 U.S.P.Q.2d 1313, 1318 (Federal Circuit 2000) (citations omitted, italics in original, emphasis added)).

In addition, it would be also improper to later suggest that the claimed features are inherent in the above situation. To suggest such, there will need to be provided a "basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristics *necessarily* flows from the teachings of the applied art." (See M.P.E.P. § 2112; emphasis in original; and see *Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Int'f. 1990)). Thus, the M.P.E.P. and the case law make clear that simply because a certain result or characteristic may occur in the prior art does not establish the inherency of that result or characteristic.

Accordingly, Applicants respectfully submit that claims 8 to 18 are allowable over the references; and withdrawal of the rejection of claims 8 to 18 under 35 U.S.C. § 103(a) is respectfully requested.

In summary, it is respectfully submitted that all of claims 8 to 18 of the present application are allowable for the foregoing reasons.

CONCLUSION

In view of all of the above, it is believed that the rejections of claims 8 to 18 under 35 U.S.C. § 103(a) has been overcome. Accordingly, it is respectfully submitted that all claims 8 to 18 are allowable. It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

In addition, it is respectfully submitted that the final nature of this Office Action is

improper and contrary to the Patent Rules; thus, the finality of this Office Action should be withdrawan.

If it would further allowance of the present application, the Examiner is invited to contact the undersigned at the contact information given below.

Respectfully submitted, Reg. No. 47084

Dated: May 19, 2004

By: Richard L. Mayer (Reg. No. 22,490)

CUSTOMER NO. 26646

KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200